Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error

Mrs. Musale Shital Satapa[1], Prof. S. S. Pawar[2]

[1]*M.E. Student of Bharati Vidyapeeth, College of Engineering Kolhapur, Shivaji University*

[2]*Asst. Professor Bharat Vidyapeeth ,College of Engineering Kolhapur, Shivaji University*

Abstract: In the today's world transfer of data over the network increases tremendously. So, the security of data is Very important for secure communication. The Steganography is a technique in which the data is hidden in the multimedia content like image, audio, video. The Cryptography alone is not sufficient for securing the data. So, in this paper we use the concept of data security using Steganographic SLSB algorithm. This paper deals with data hiding in compressed Video. Motion vectors are calculated using macro block prediction error, which is different from the approaches Based on the motion vector attributes such as the magnitude and phase angle, etc. Information hiding is a method of hiding secret data into a host medium so that the hidden data are imperceptible but known to the intended recipient [1]. The host medium may be a digital image, audio, video, or another type of media. Among the different kinds of media, the digital image is most popularly used as the host media to convey secret information. In the image hiding system, the image used to embed secret data is called the host image (cover image). The resultant image, which is embedded with secret data, is called the stego-image.

Keyword: Steganography, LSB, motion vectors.

1 INTRODUCTION

Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent un authorized copying directly[5]. Military communications systems make increasing use of traffic security techniques which, rather than merely concealing the Content of a message using encryption; seek to conceal its sender, its receiver or its very existence. Similar techniques are used in some mobile phone systems and schemes proposed for digital elections. First cover data is divided in to frames .Find out motion vectors using motion estimation method. Then secrete data is modified using a secrete key. The secrete data is embedded in a cover medium by using a LSB method.

2. SYSTEM MODEL

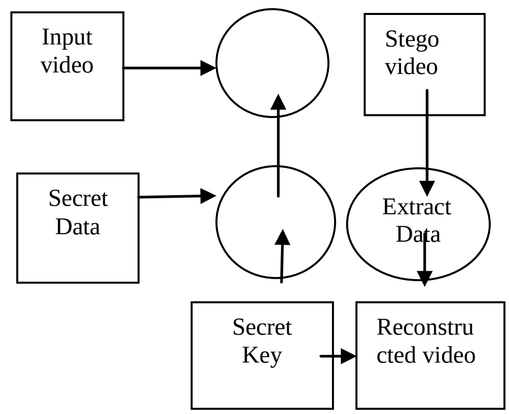

Figure: 1 Data hiding technique

The above figure shows data hiding technique in compressed video. The input video is separated into frames. Then the frames are subjected to DCT and Huffman coding to compress the frame. Using the secret key and LSB algorithm data is inserted. This generated video is stego video. The secret data can be extracted using inverse LSB and secret key[5].

3. PREVIOUS WORK

In [1] least significant bit algorithm is used for hiding the secret data by identifying the motion vectors based on their associated macro block prediction error. In [2] video data hiding techniques extended to video by hiding the message in each frame independently. Methods such as spread spectrum are used, where the basic idea is to distribute the message over a wide range of frequencies of the host data. In [3] and [4] the data bits of the message are hidden in some of the motion vectors whose magnitude is above a predefined threshold, and these motion vectors are called as candidate motion vectors. A single bit is hidden in the least significant bit of the larger component of each candidate motion vector. The authors in [7] and [8] embed the data in video using the phase angle between two consecutive candidate motion vectors. These candidate motion vectors are selected based on the magnitude of the motion vectors as in [2].The message bit stream is encoded as phase angle difference in sectors between candidate motion vectors. The block matching is constrained to search within the selected sector for a magnitude to be larger than the predefined threshold.

4. PROPOSED METHODOLOGY

The following figure shows data hiding technique in compressed video. The input video is separated into frames. Then the frames are subjected to DCT and Huffman coding to compress the frame. Using the secret key and LSB algorithm data is inserted.This generated video is stego video. The secret data can be extracted using inverse LSB and secret key. In this section, the general operations of data hiding by simple LSB substitution method are described.

LSB Algorithm

Input: Video

Output: Stego video

Step 1: Read the input Video

Step 2: Perform frame separation

Step 3: Apply Integer DCT on each 8×8 block.

Step 4: Perform Zigzag Scanning on each 8×8

Block.

Step 5: Apply Huffman coding to compress the frame.

Step 6: Apply secret key to hide the data.

Step 7: Apply LSB Algorithm to embed data

Step 8: Generate Stego video

Algorithm for Extraction Process

Input: Stego video

Output: Hidden data

Step 1: Read Stego video.

Step 2: Perform decoding using IDCT and Inverse

Huffman coding.

Step 3: Extract hidden data using ILSB and Secret Key.

5. EXPERIMENTAL RESULTS

We implemented the hiding and extraction Algorithms and integrated them to the MPEG-2 encoder and decoder operation. The parameters of our experiments, presented in this section, are: macro block size b=16 motion vector representation bits n=5. We used fast three-steps motion estimation algorithms with half pixel accuracy. Each test video sequence is organized into consecutive GOP organized as [I,B,B,P,B,B,P,B,B.] We tested our algorithms on two standard test sequences: car-phone, foreman which are all shown in Fig.1. The foreman have a frame size of 352*288 which corresponds to 396 macroblocks per frame. The number of macroblocks per frame and the total number of frames for each sequence are given in the first column of Table 1 & 2. The motion estimation method used is given in the second column of Table 1 & 2. Thus we performed 12 different experiments on natural video sequences with different levels of motion. Foreman and car-phone sequences have an almost static background with human face motion at the foreground. Our algorithm may hide a maximum of (2*B)/8 bytes per P-frame and (4*B)/8 per B-frame. Analyzing the PSNR values of the prediction error E_r for all sequences, we set T_{max} =60 dB and T_{min} =20 dB for P-frames, and T_{max} = 40,T_{min} =15dB for B-frames.

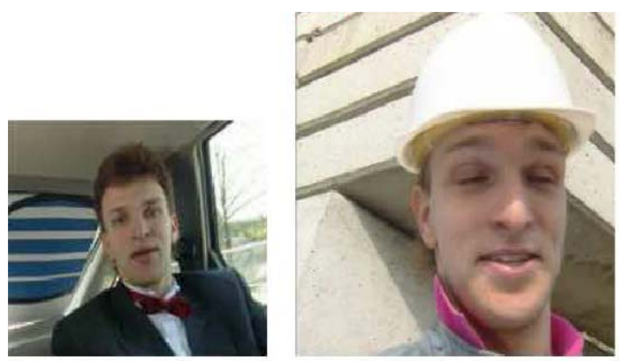

Fig.2.First image of test sequences: a) Car-Phone, b) Foreman

We evaluated our algorithm and compared it to an attribute-based method [4] which is dependent on a threshold T of the magnitude of the motion vectors. We have chosen the threshold T for [4] that produces the closest total number of embedded bytes (payload) to that of our algorithm for the whole test sequence.

Table1: Quantitative performance measures ∆R, ∆D of our Method

Test Sequence	Motion estimation search method	Total payload (Bytes)	Average ∆R per frame	Total ∆D (Byte)
Carphone(99B/frame)(270frames=30GOP)	Three step search	4811	-0.325	10645
Foreman(396B/frame)(135frames=17 GOP)	Three step search	6577	-0.244	30379

Table 2: Quantitative performance measures ∆R, ∆D of Method in 4.

Test Sequence	Motion estimation search method	Total payload (Bytes)	Average ∆R per frame	Total ∆D (Byte)
Carphone(99B/frame)(270frames=30GOP)	Three step search	3995(T=0.5)	-0.560	28148
Foreman(396B/ frame) (135frames=17 GOP)	Three step search	5722(T=1.5)	-0.346	861818

The payload for both methods and the associated threshold T in values of pixels for [4] are shown in the first column of each method's results in Table 1.For each sequence we calculated the average over all frames for the drop in PSNR Δ^R which indicates the quality degradation of the reconstructed video in effect to the hiding; Δ^R are shown in the second columns for both methods' results. Finally, the data size increase due to hiding the data is measured for each frame and the total data size increase for all frames are given in the third column of the results of both methods. Analyzing the results in Table 1, we find that for approximately the same payload, our hiding method produces less distortion to the video as $-\Delta^R/$ total payload is smaller than that in [4] and generally the distortion is less than 0.6 dB which is nearly invisible. The effect on the data size increase is less than that in [4] which is accounted for our hiding criteria that selects those whose prediction error is high and refrain from tampering those associated with low error.

6 . CONCLUSION

We proposed a new data-hiding method in the motion vectors of MPEG-2 compressed video. Unlike most data-hiding methods in the motion vectors that rely their selection on attributes of the motion vectors, we chose a different approach that selects those motion vectors whose associated macro blocks prediction error is high (low PSNR) to be the candidates for hiding a bit in each of their horizontal and vertical components. A greedy search for the suitable value of the threshold to be used for choosing the macro blocks corresponding to the CMV is done such that the candidates will be identically identified by the decoder even after these macro blocks have been lossy compressed. The embedding and extraction algorithms are implemented and integrated to the MPEG-2 encoder/decoder and the results are evaluated based on two metrics: quality distortion to the reconstructed video and data size increase of the compressed video. The method is compared to another one from the literature that relies on a motion vector attribute. The proposed method is found to have lower distortion to the quality of the video and lower data size increase.

7. FUTURE SCOPES

This method is compared to another one from the literature that relies on a motion vector attribute. The proposed method is found to have lower distortion to the quality of the video and lower data size increase. Future work will be directed towards increasing the size of the embedded payload while maintaining the robustness and low distortions

REFERENCES

[1] Hussein A. Aly ―Data Hiding in Motion Vectors of Compressed Video Based on Their Associated Prediction Error‖ IEEE Trans On Information Forensics And Security, Vol. 6, No. 1, Mar 2011.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, Information hiding—A survey,‖ Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.

[3] J. Zhang, J. Li, and L. Zhang, ―Video watermark technique in motion vector,‖ in Proc. XIV Symp. Computer Graphics and Image Processing, Oct. 2001, pp. 179–182
[4] C. Xu, X. Ping, and T. Zhang, "Steganography in compressed video stream," in Proc. Int. Conf. Innovative Computing, Information and Control (ICICIC'06), 2006, vol. II, pp. 803–806.
[5] "A Secure Data Hiding Technique in Compressed Video Using a Secret Key " V. Manjula, J.Rajani, K.Radhika Asst.Prof, Dept of CSE. Institute of Aeronautical Engg Hyderabad, India
[6] D.-Y. Fang and L.-W. Chang, "Data hiding for digital video with phase of motion vector," in Proc. Int. Symp. Circuits and Systems (ISCAS), 2006, pp. 1422– 1425 .
[7] X. He and Z. Luo, "A novel steganographic algorithm based on the motion vector phase," in Proc. Int. Conf. Comp. Sc. and Software Eng., 2008, pp. 822–825 .
[8] Generic Coding of Moving Pictures and Associated Audio Information: Video, 2 Edition, SO/IEC13818-2, 2000.

AUTHOR'S PROFILE

Mrs. Shital Satapa Musale has received my Bachelor of Engineering degree in Electrical & Electronics Engineering from Bharati Vidyapeeth College of engineering Kolhapur in year 2011.At present I doing M.E. From same college with specialization in Image processing.

Prof. Sanjay S. Pawar doing a job as a lecturer in Bharati vidyapeeth college of engineering Kolhapur. He appeared for P.H.D.